Moorland
Waldorf School

E-Safety Policy

Policy Reviewed: November 2021
Next Policy Review Date: November 2022

Introduction

MWS is dedicated to nurturing each child's capacity for creative imagination, independent thinking and positive action. The school's efforts to foster pupils' healthy emotional development and meaningful relationships with their environment are undermined by those encounters with media that separate children from authentic experience and promote a distorted, developmentally inappropriate and consumerist view of the world. Pupils' best learn to use electronic media as a resource and tool when these media are introduced after children have developed a rich experiential foundation. Media thus becomes a supplement to, not a substitute for, the richness of direct experience.

The school asks that parents' guide their children in the appropriate uses of electronic media outside of the school environment. We encourage parents to keep an open dialogue with their children, other class parents, teachers and advisor regarding media. Specifically, parents should speak to teachers—either privately or with other parents in class or other group meetings—about their questions and challenges related to media so that together they can work out viable approaches.

Access to the Internet

The use of the internet can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content;
- Unauthorised access to / loss of / sharing of personal information;
- The risk of being subject to grooming by those with whom they make contact on the internet;
- The sharing / distribution of personal images without an individual's consent or knowledge;
- Inappropriate communication / contact with others, including strangers;
- Cybersquatting;
- Access to unsuitable video / internet games;
- An inability to evaluate the quality, accuracy and relevance of information on the internet;
- Plagiarism and copyright infringement;
- Illegal downloading of music or video files;
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

When children are using computers they are to be sited in areas of high visibility which will enable children, young people and adults to be closely supervised and their online use to be appropriately monitored.

Links with other Policies

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. Behaviour, Anti-bullying and Child Protection Policies). Any incidents of cyber bullying or other e safety incidents listed in this policy which occur outside of school will still be dealt with in school in line with other polices such as the behaviour policy, child protection policy, the anti-bullying policy. Parent/carers will be informed of such behaviour even if it is out of school.

Education

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

MWS will ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks.

Staff alongside parents and carers, should consider it to be their duty to make children and young people aware of the potential risks associated with online technologies. This will empower them with the knowledge and skills to keep safe, without limiting their learning opportunities and experiences.

'E-safety' will taught to children, in age appropriate way, from Kindergarten. The school will also offer e-safety training/ awareness evenings for parents on an annual basis. Staff should reinforce e-safety messages in the use of ICT to all pupils when using computers with them.

This policy applies to all staff and students and anyone using the school internet system.

Advice for students:

- Don't publish identifying information.
- Pick a user name that doesn't include any personal information.
- Set up a separate email account that doesn't use your real name and use that to register and receive mail from the site. That way if you want to shut down your connection, you can simply stop using that mail account.
- Use a strong password (at least 8 characters; mixture of lower case letters, upper case letters, numbers and symbols).
- Keep passwords safe, and change them regularly.
- Keep your profile closed.
- Only allow friends to view your profile.
- What goes online stays online. Don't say anything or publish pictures that might cause you embarrassment later. If you wouldn't say it to your parents, don't say it online!
- Be on your guard.
- Talk to parents/carers if you feel uncomfortable.
- Save or print evidence.

Advice for Parents

- Set ground rules. Discuss. Continue to talk.
- Limit the amount of time online.
- Use ISP filtering.

- Set up a family e-mail account for registering on websites, competitions etc.
- Monitor online activity (recently visited sites, click the History button).
- Software for filtering isn't fool proof -combine with supervision.
- Check temporary files (open Internet Explorer and select Internet Options, on the General tab under Temporary Internet Files, click the Settings button and the click View Files).
- Contact CEOP or the police if you suspect grooming.

CEOP (Child Exploitation & Online Protection) is dedicated to eradicating the sexual abuse of children, and is affiliated to the Serious Organised Crime Agency (SOCA).

Safer search engines:

- surfsafely.com
- askkids.com
- yahookids.com

Further information and advice:

- childnet.com (select 'Know It All' for a wide range of links to other sites)
- google.co.uk/goodtoknow (select 'Stay safe online')
- getsafeonline.org
- kidscape.org.uk
- mydaughter.co.uk

Useful information can also be found at:

https://www.gov.uk/government/publications/preventing-and-tackling-bullying

Control Measures

The following control measures will be put in place which will manage internet access and minimise risk:

- Secure broadband or wireless access.
- A secure, filtered, managed internet service provider and/ or learning platform.
- Secure email accounts.
- Regularly monitored and updated virus protection.
- A secure password system.
- An agreed list of assigned authorised users with controlled access.
- Clear Acceptable Use
- Effective audit, monitoring and review procedures.

Social Networking

It is to be recognised that staff are also likely to use social networking sites in their recreational time on their own personal computers.

This form of activity is not to be discouraged however staff must agree and adhere to a ‘professional conduct agreement’. It must be ensured that the use of such sites will not compromise professional integrity or bring the school into disrepute.

It must be recognised that social networking sites and mobile technologies can be used for negative and anti-social purposes. Cyberbullying, for example, is to be considered as unacceptable as any other form of bullying and effective sanctions must be in place to deal with such concerns. Any known or suspected incidents must be reported immediately to the Designated Safeguarding Person.

Staff must not have a pupil as a ‘friend’ or contact on any social networking medium.

Endorsement:

Name: Linda Parker
Position: Chair of ECTE
Date: 28/11/2021